

FIG.1

2/37

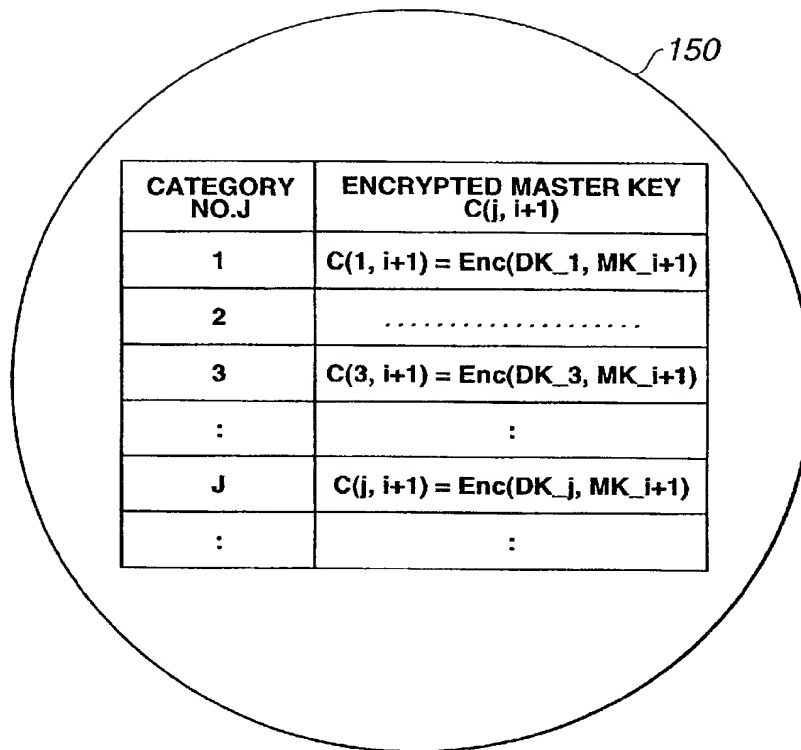


FIG.2

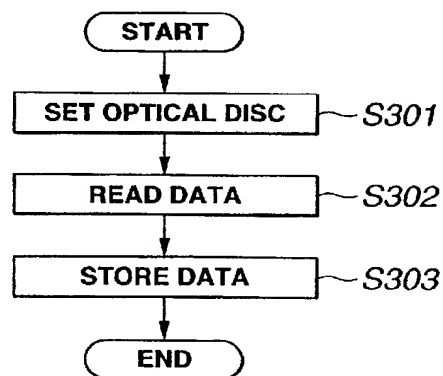


FIG.3

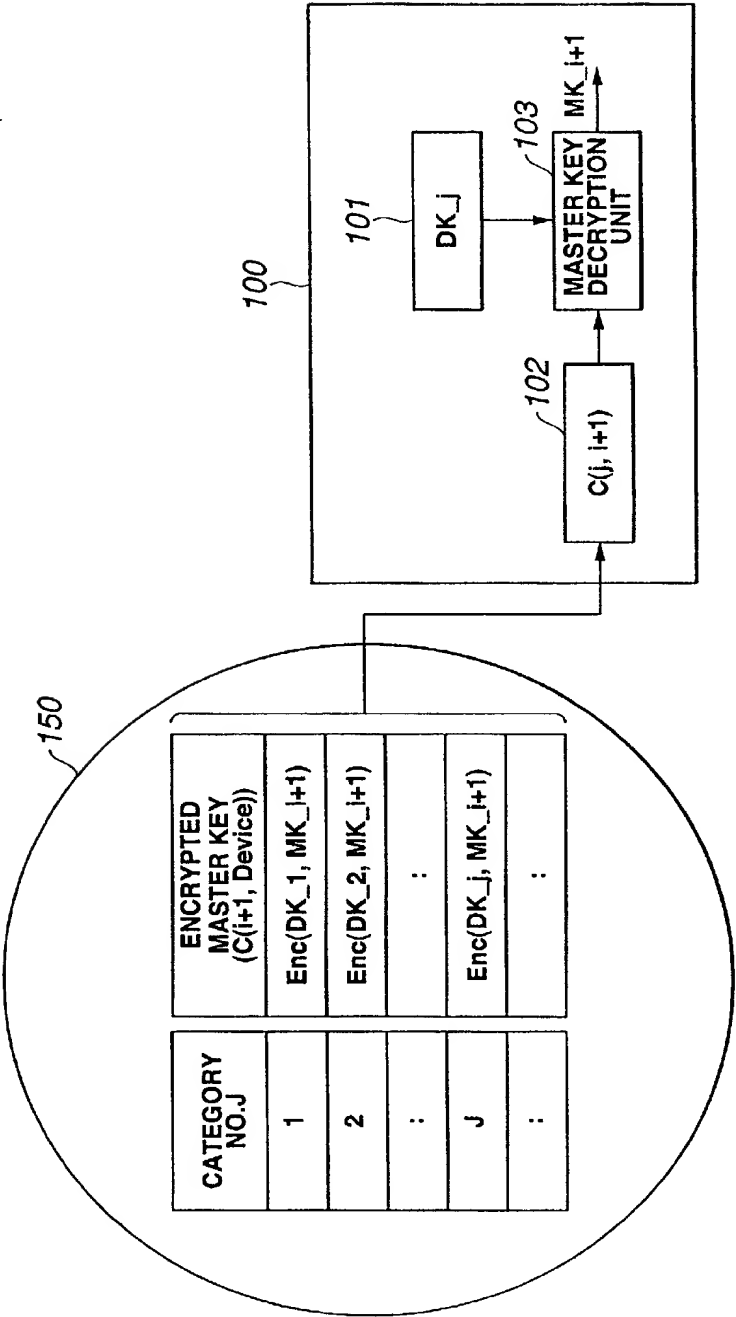
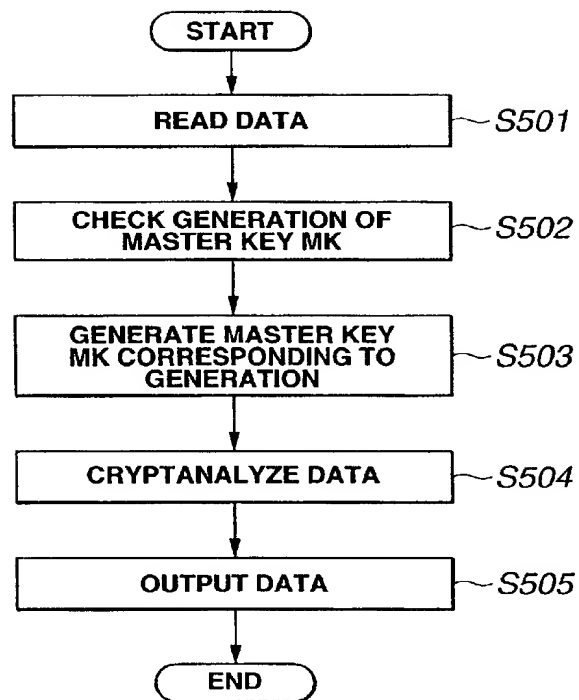


FIG.4

4/37

**FIG.5**

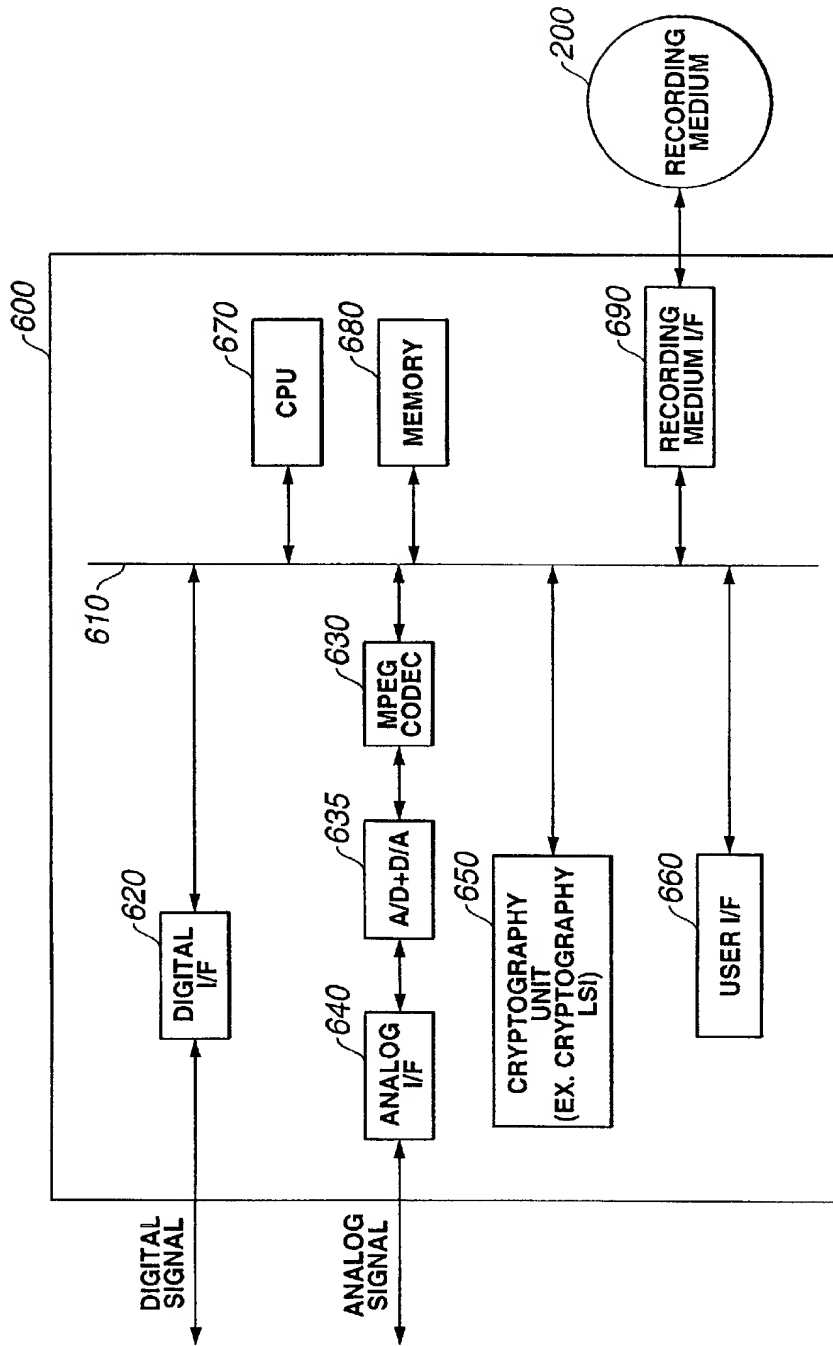


FIG.6

6/37

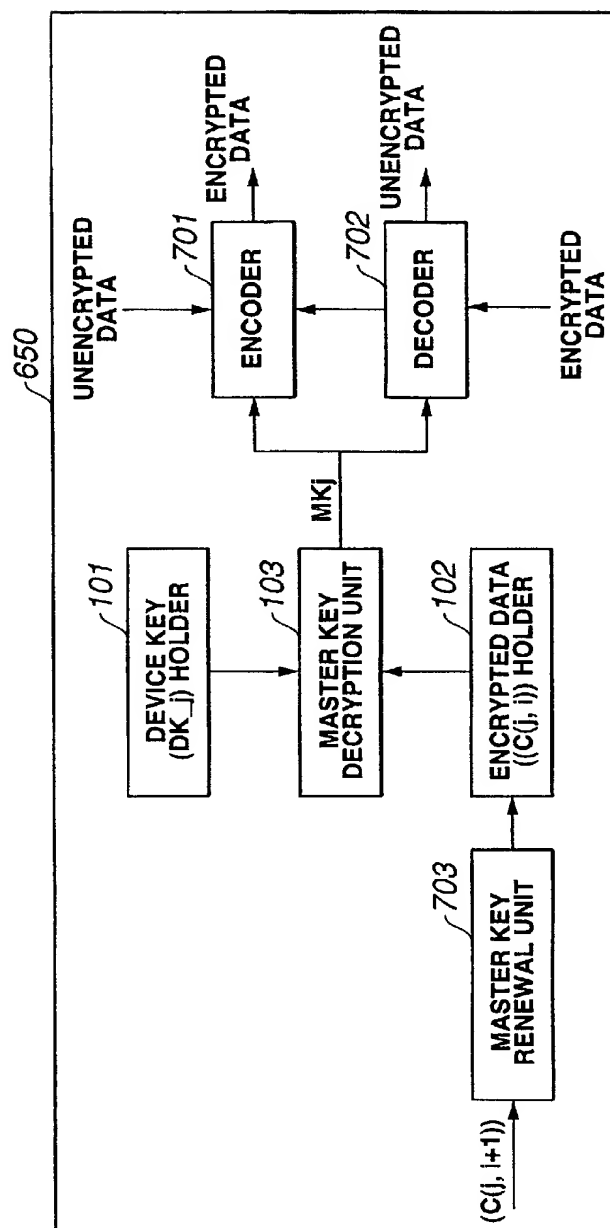


FIG.7

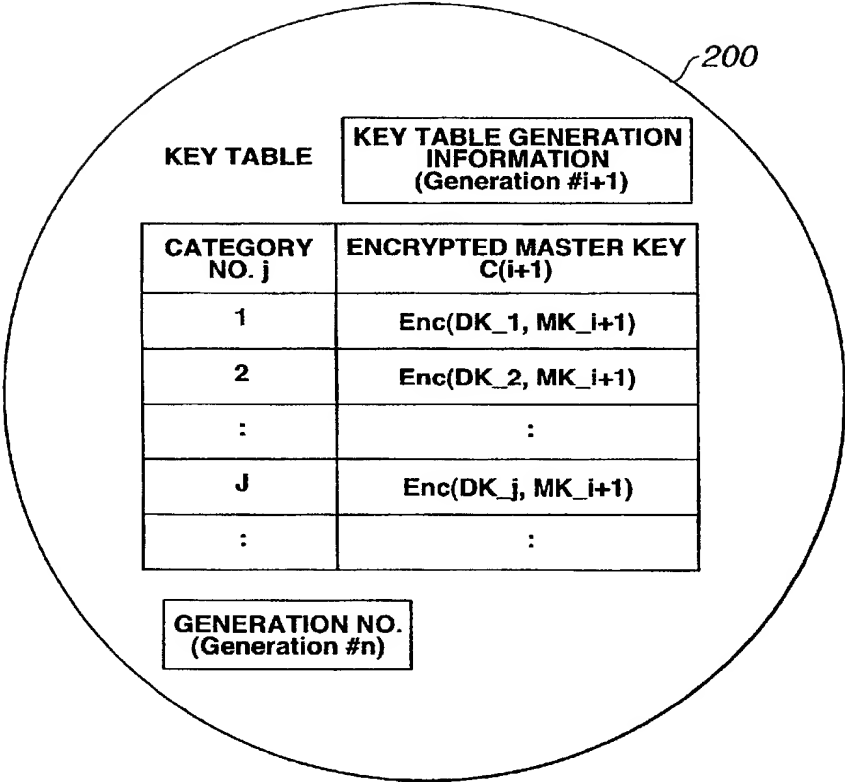


FIG.8

8/37

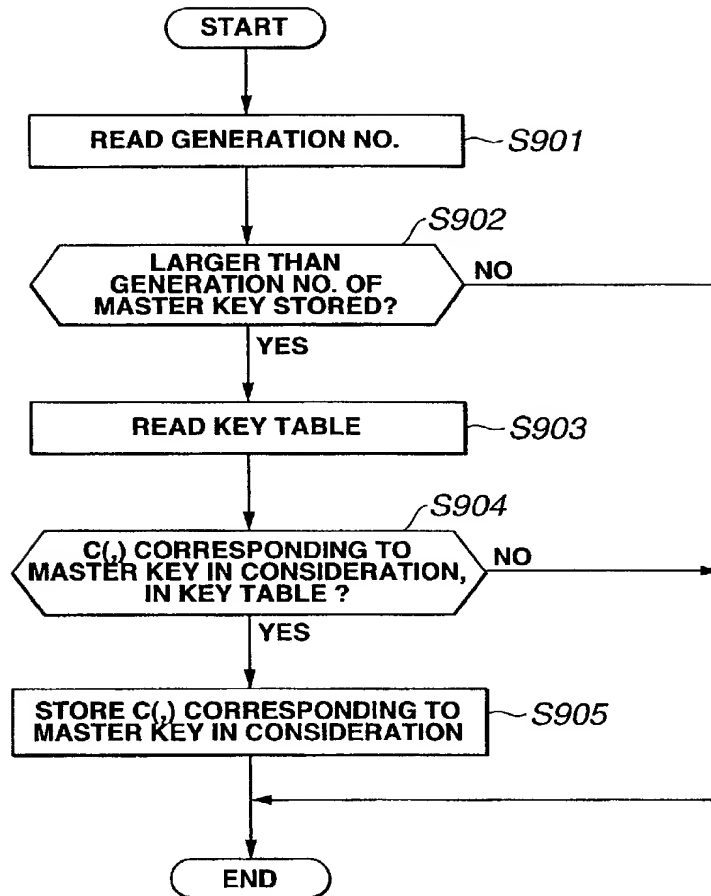
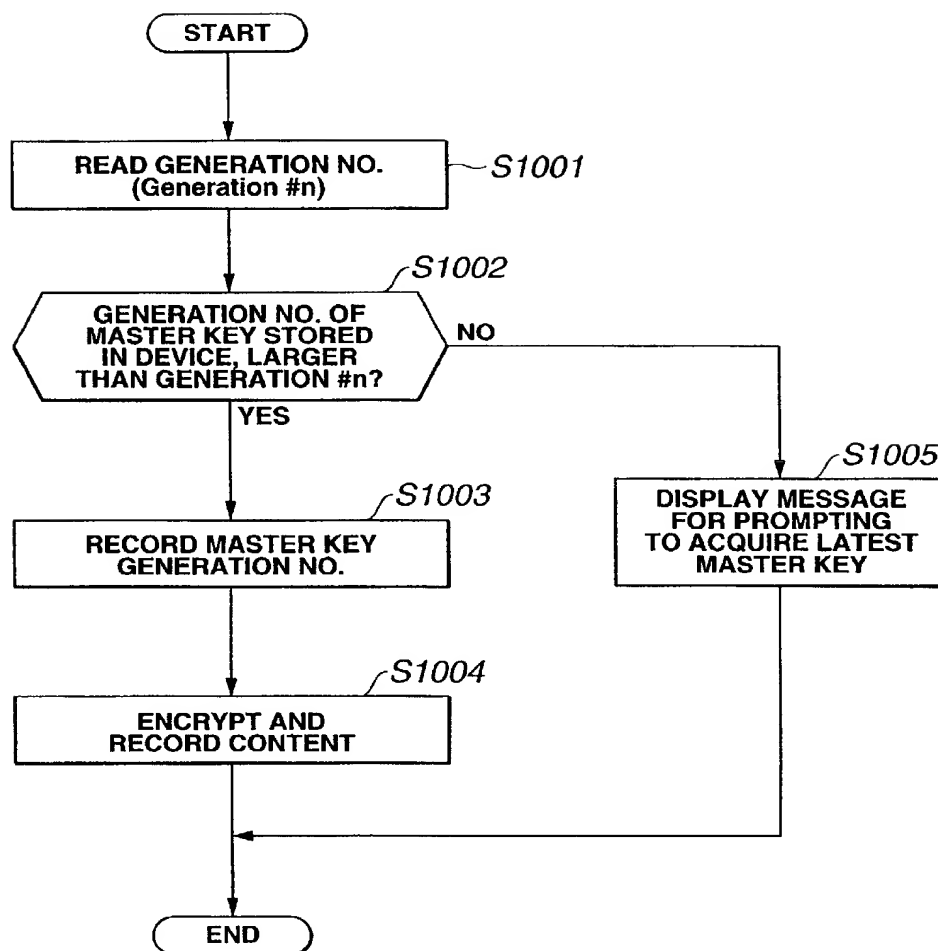


FIG.9

9/37

**FIG.10**

10/37

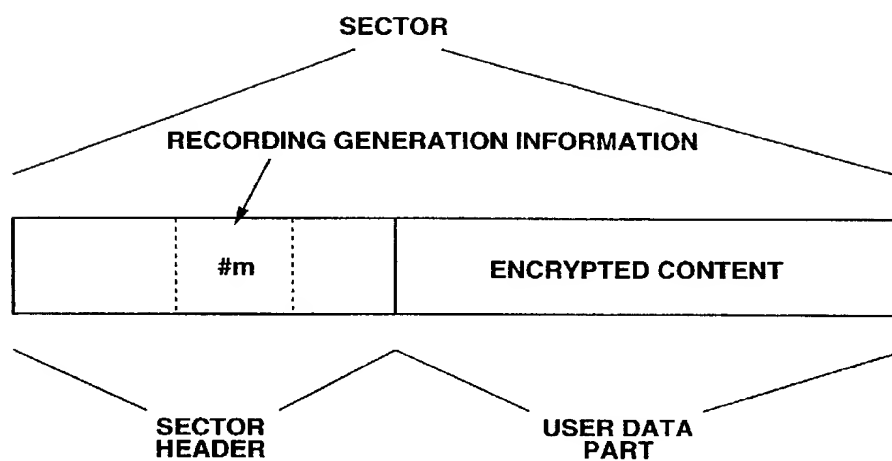


FIG.11

11/37

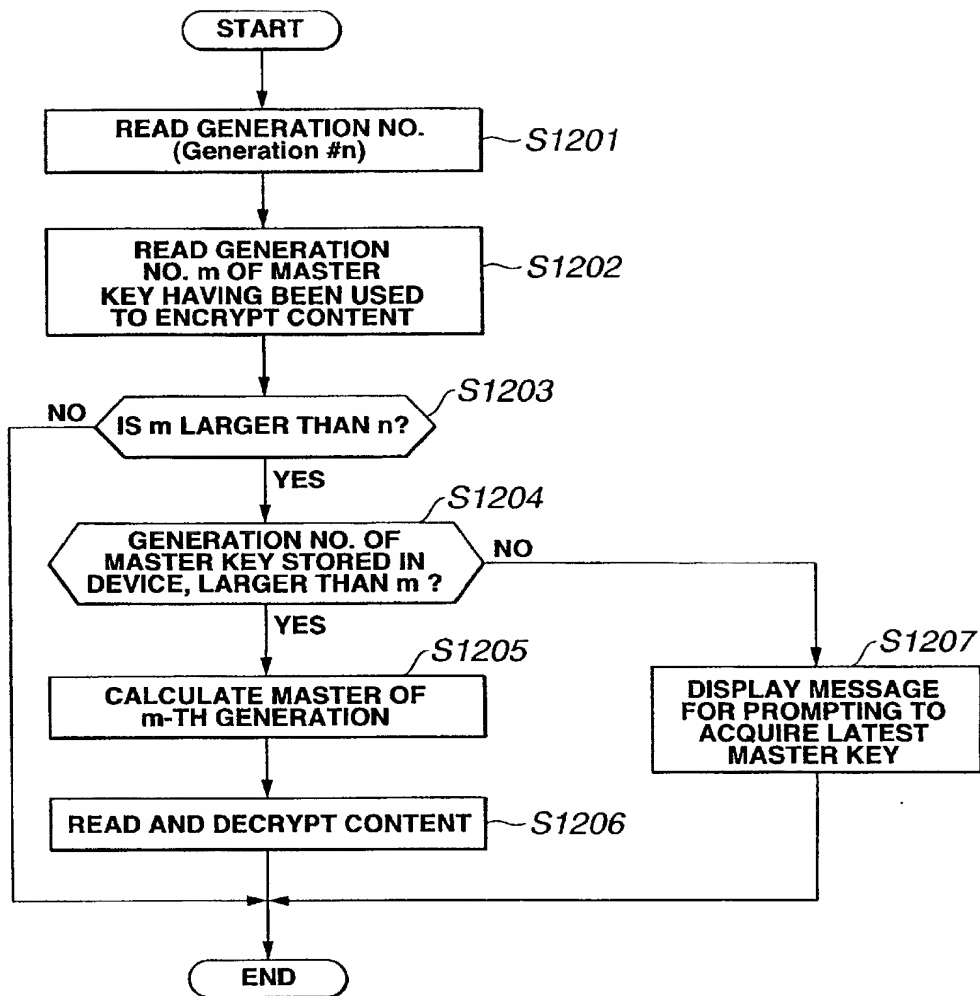


FIG.12

12/37

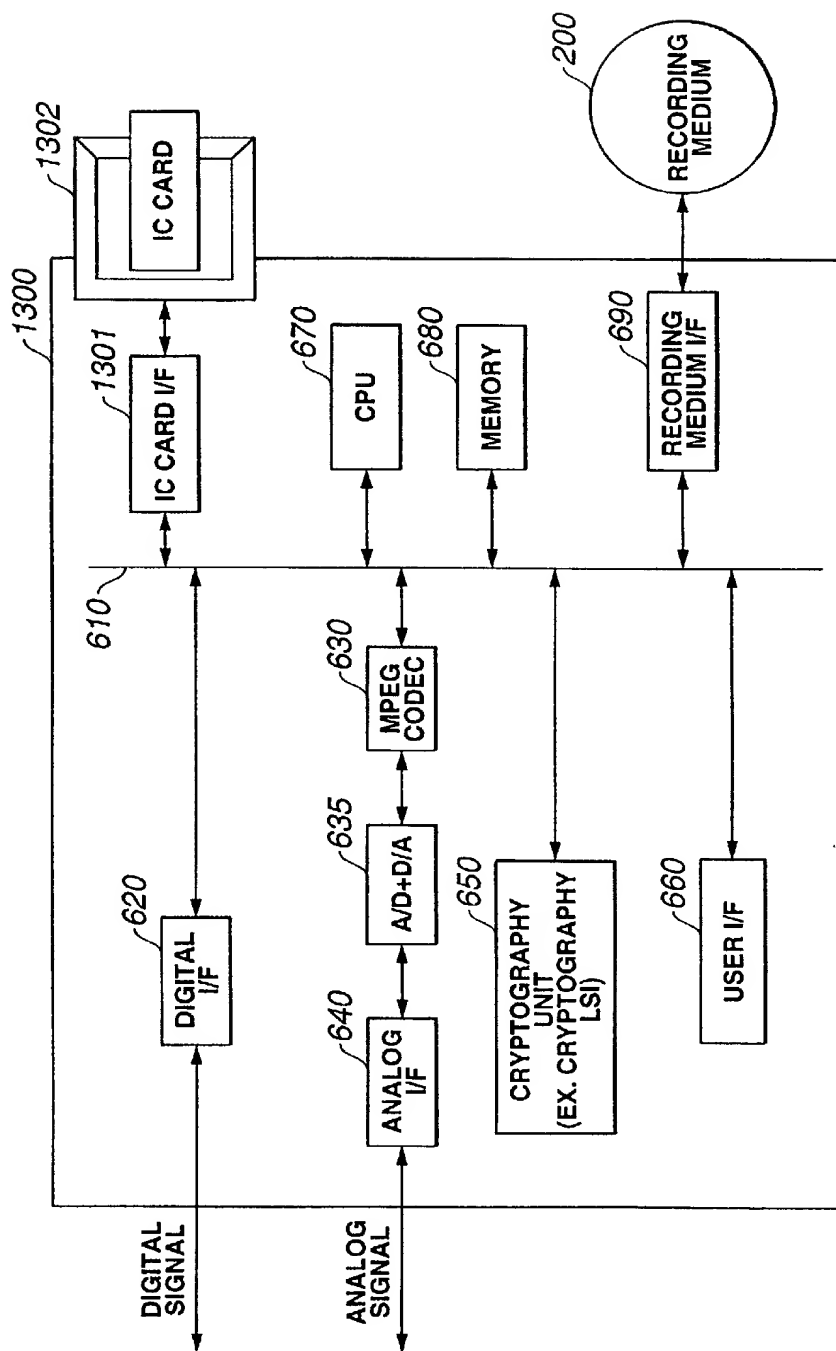


FIG.13

13/37

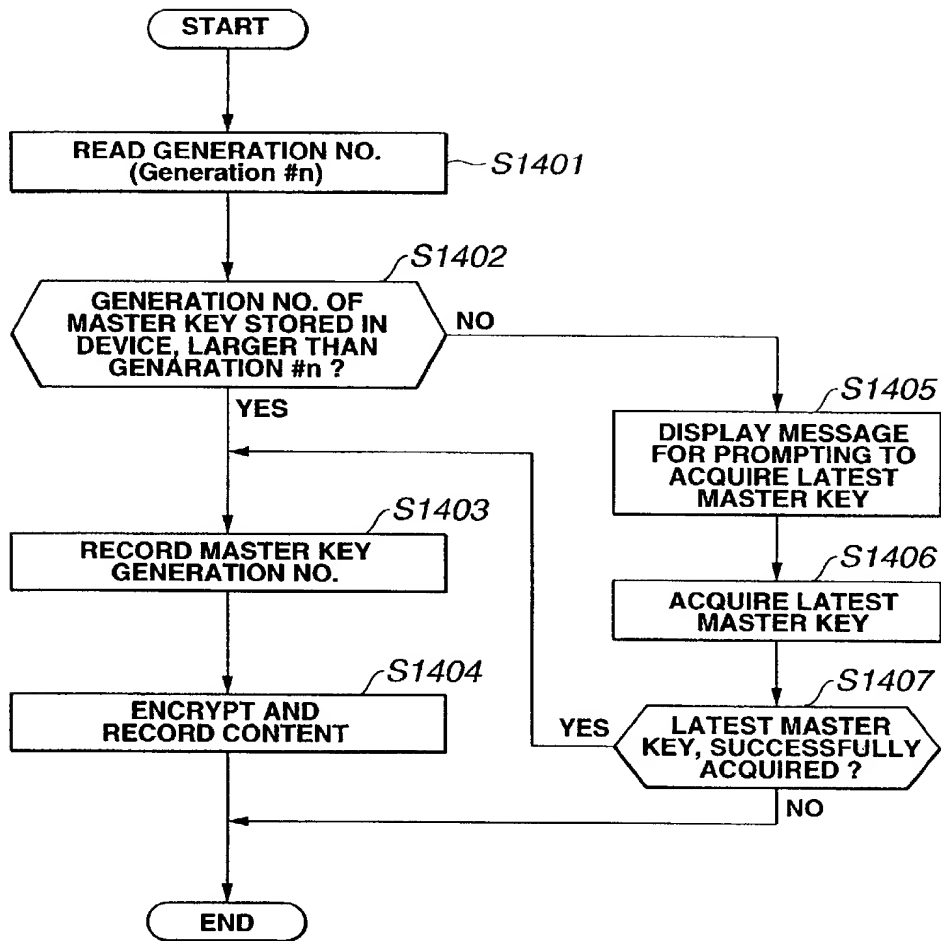


FIG.14

14/37

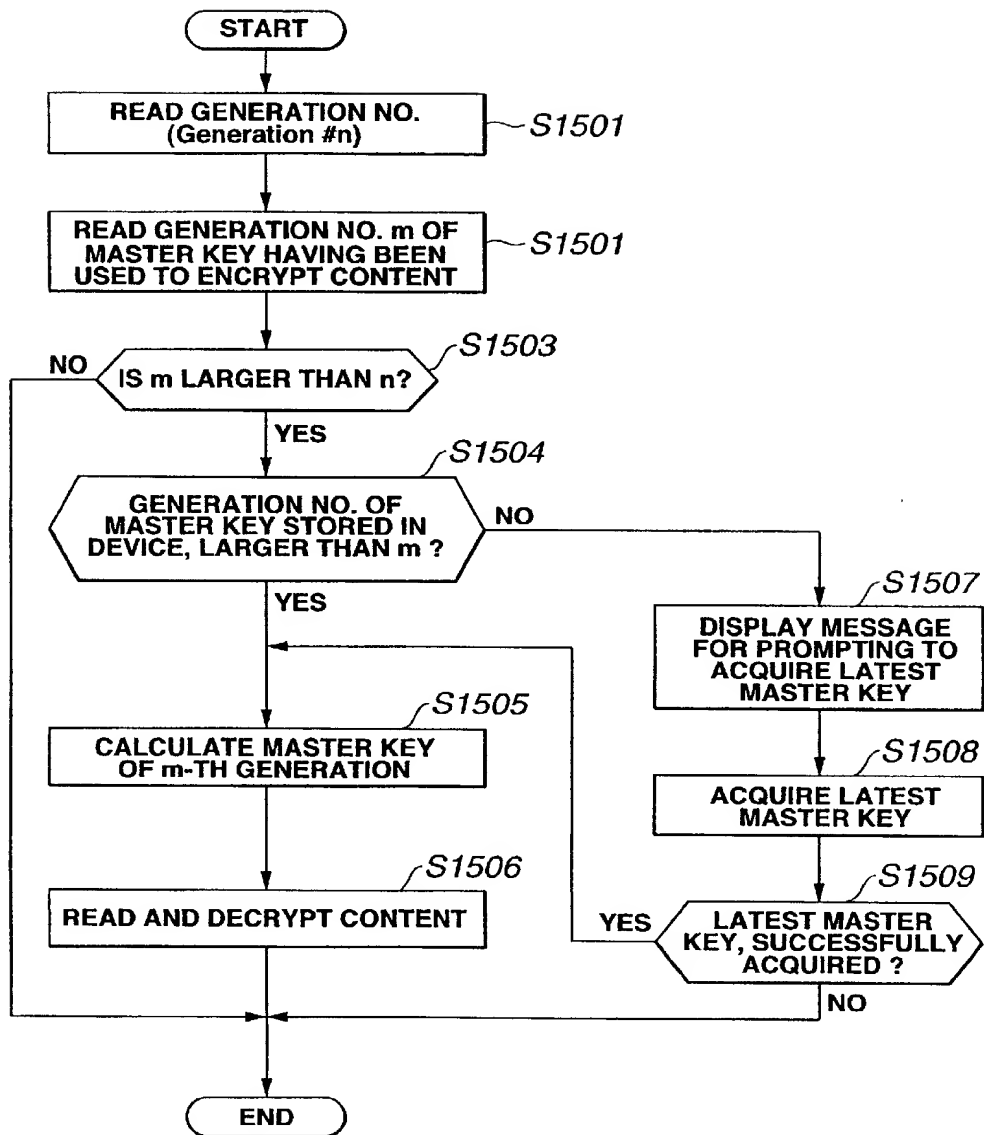


FIG.15

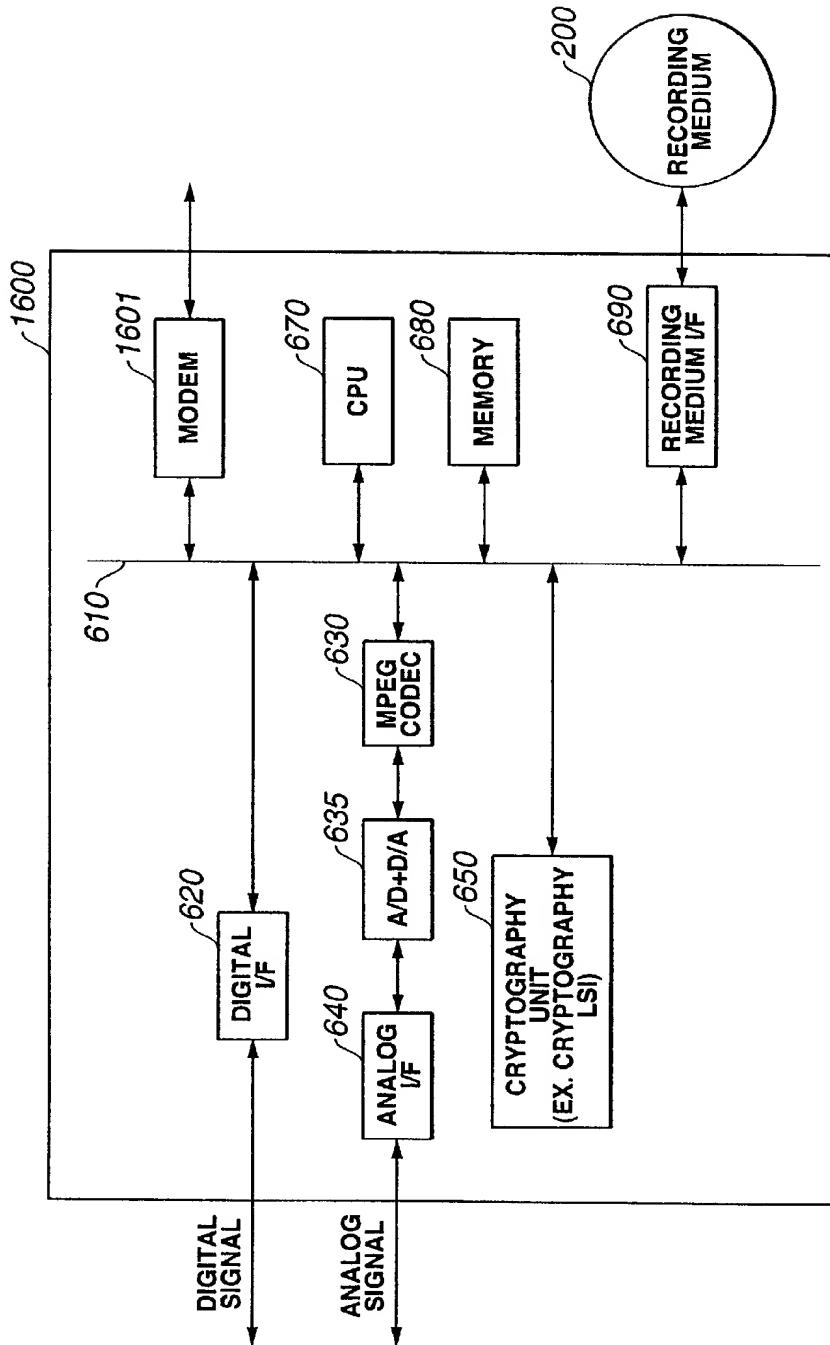


FIG.16

16/37

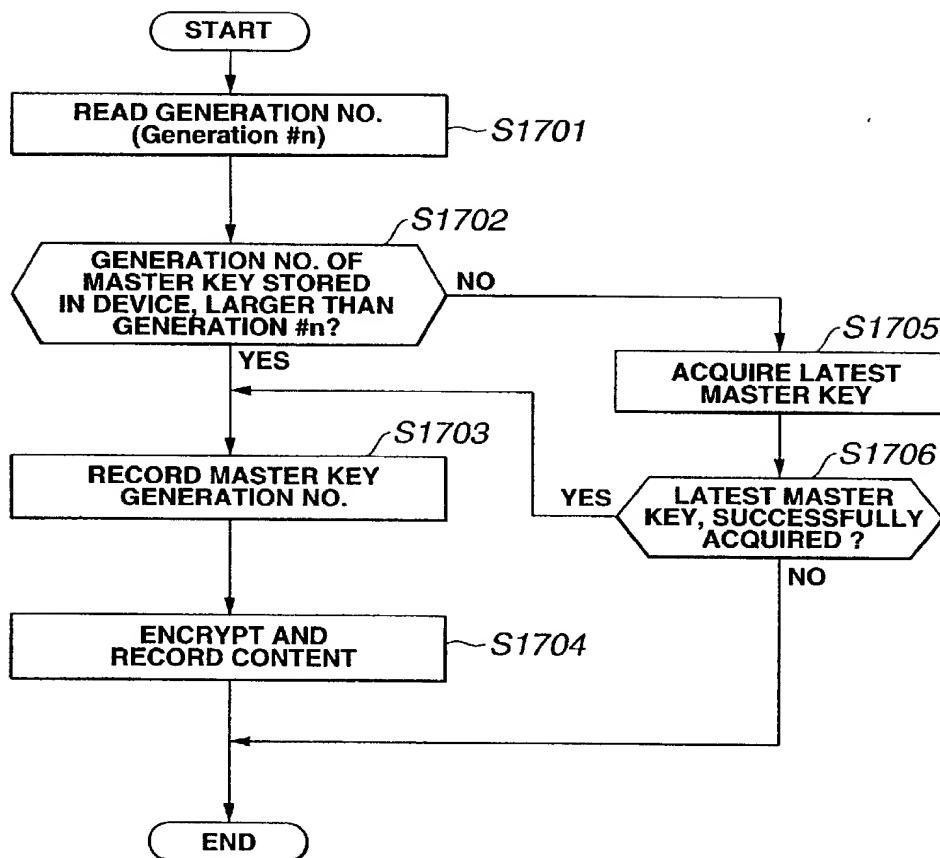


FIG.17

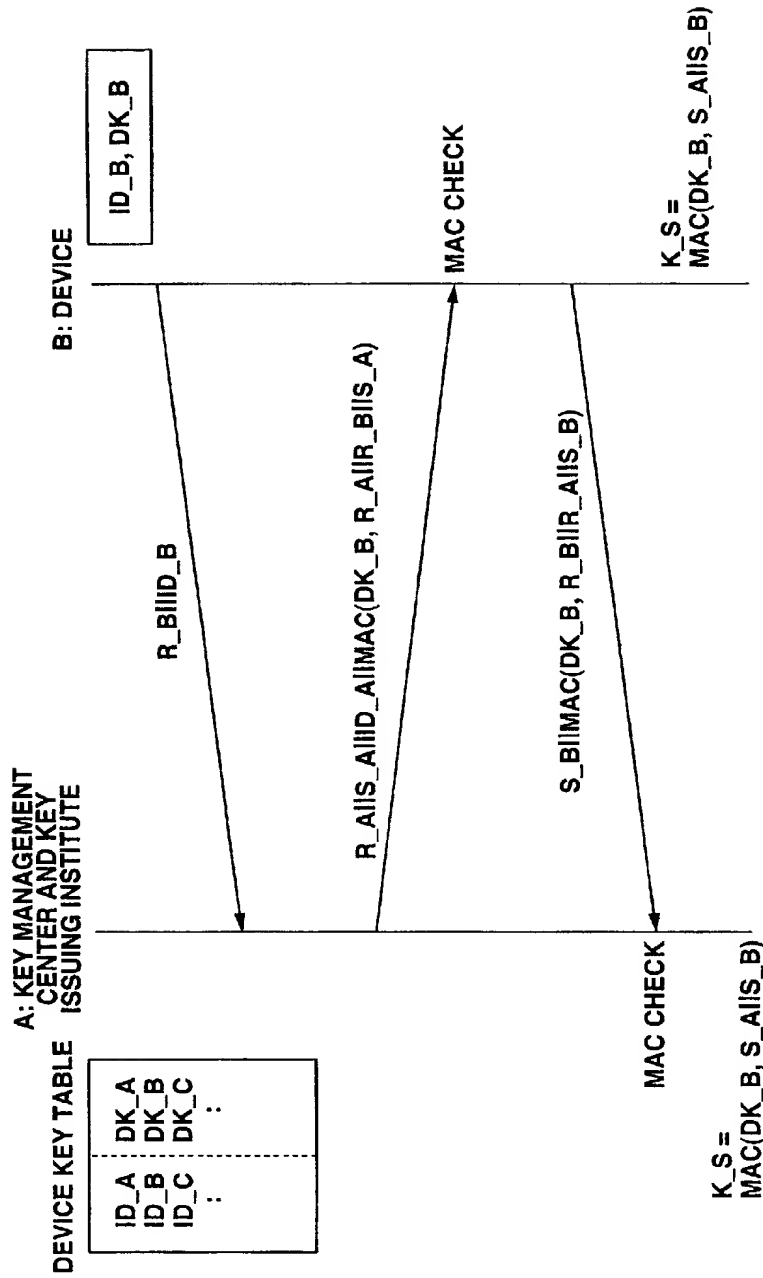


FIG.18

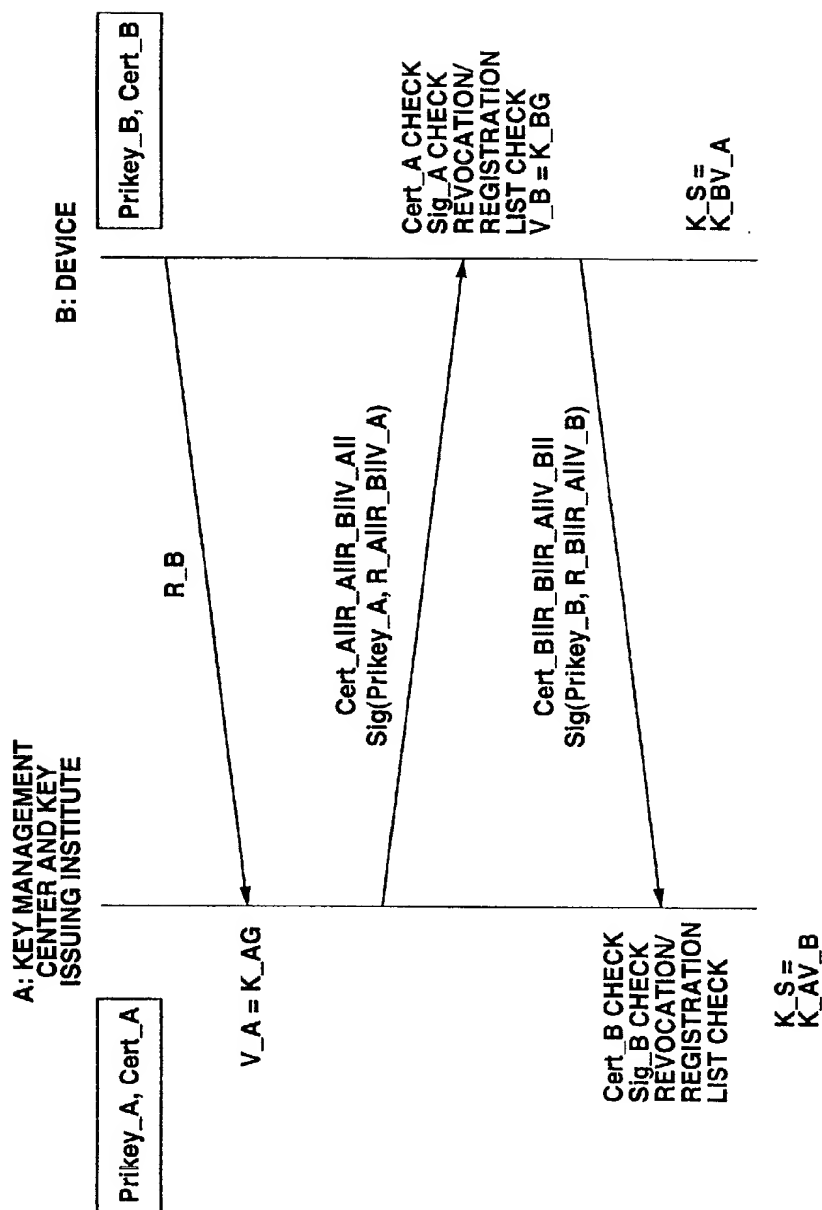


FIG.19

19/37

ID OF B (ID_B)
PUBLIC KEY OF B (Pubkey_B)
DIGITAL SIGNATURE BY CENTER TO ALL ABOVE FIELDS

**FIG.20**

VERSION NO.
ID FOR DEVICE TO BE REVOKED
:
DIGITAL SIGNATURE BY CENTER

**FIG.21**

VERSION NO.
ID OF DEVICE TO BE REGISTERED
:
DIGITAL SIGNATURE BY CENTER

**FIG.22**

20/37

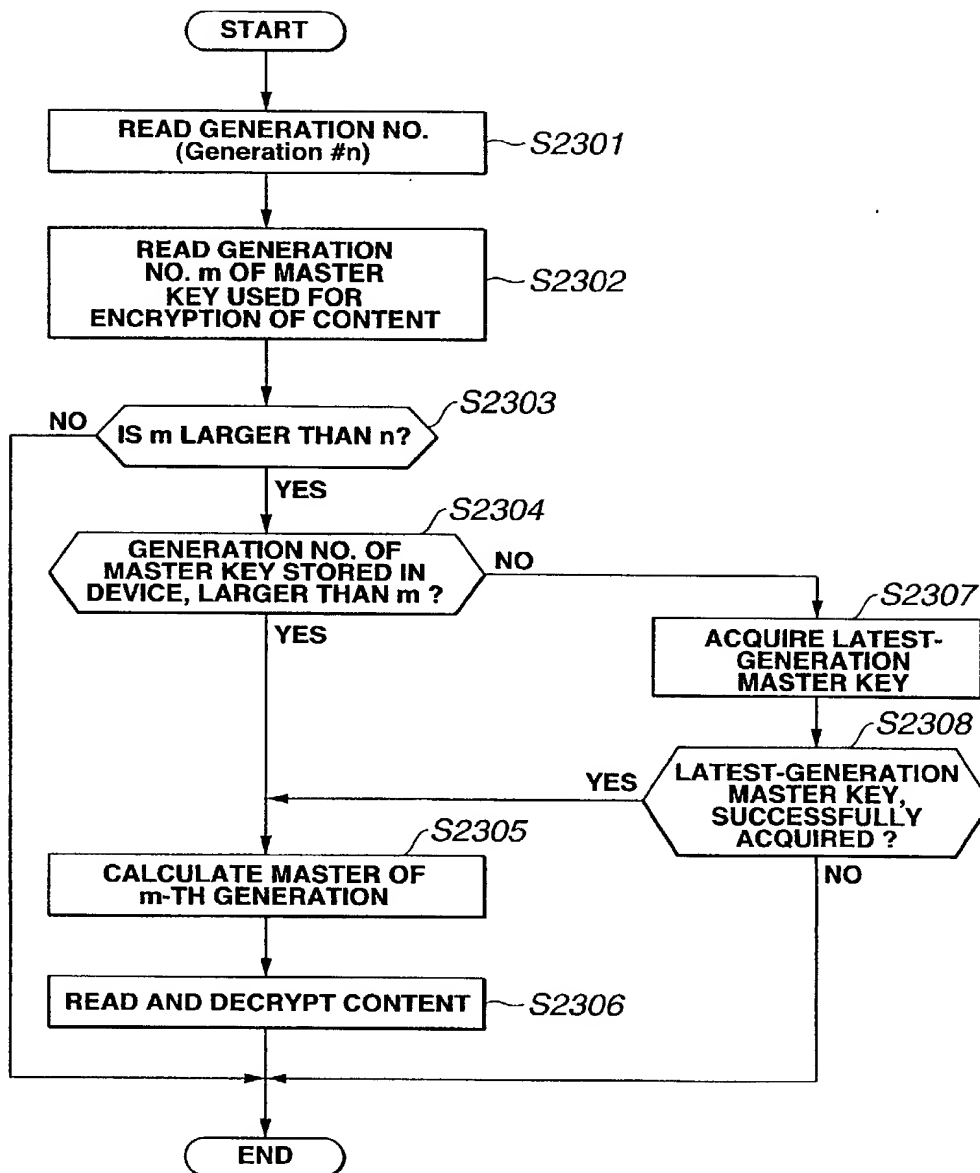


FIG.23

21/37

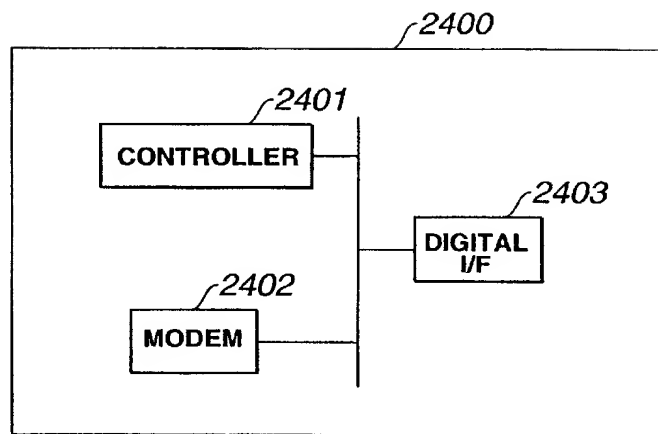


FIG.24

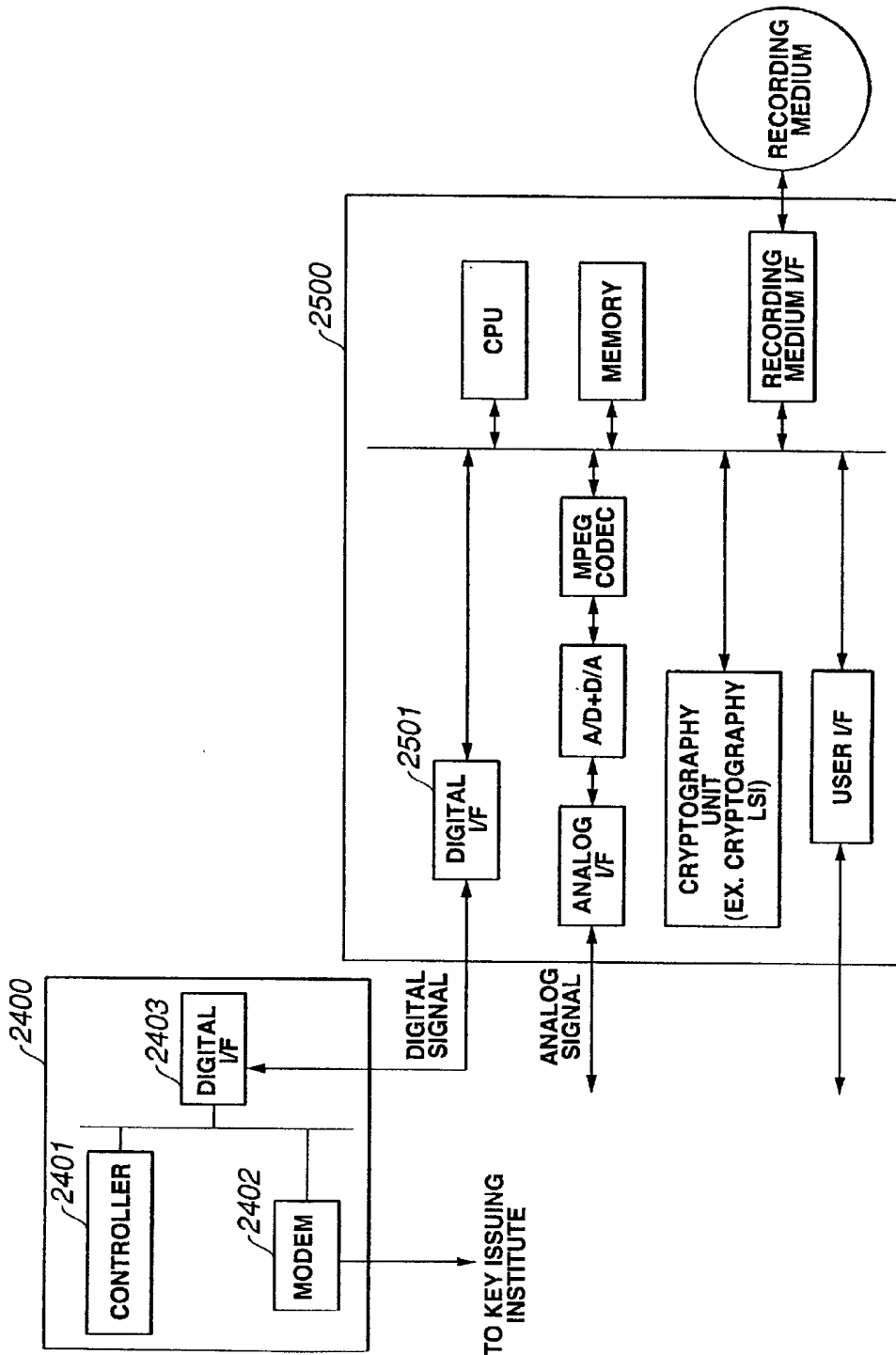


FIG.25

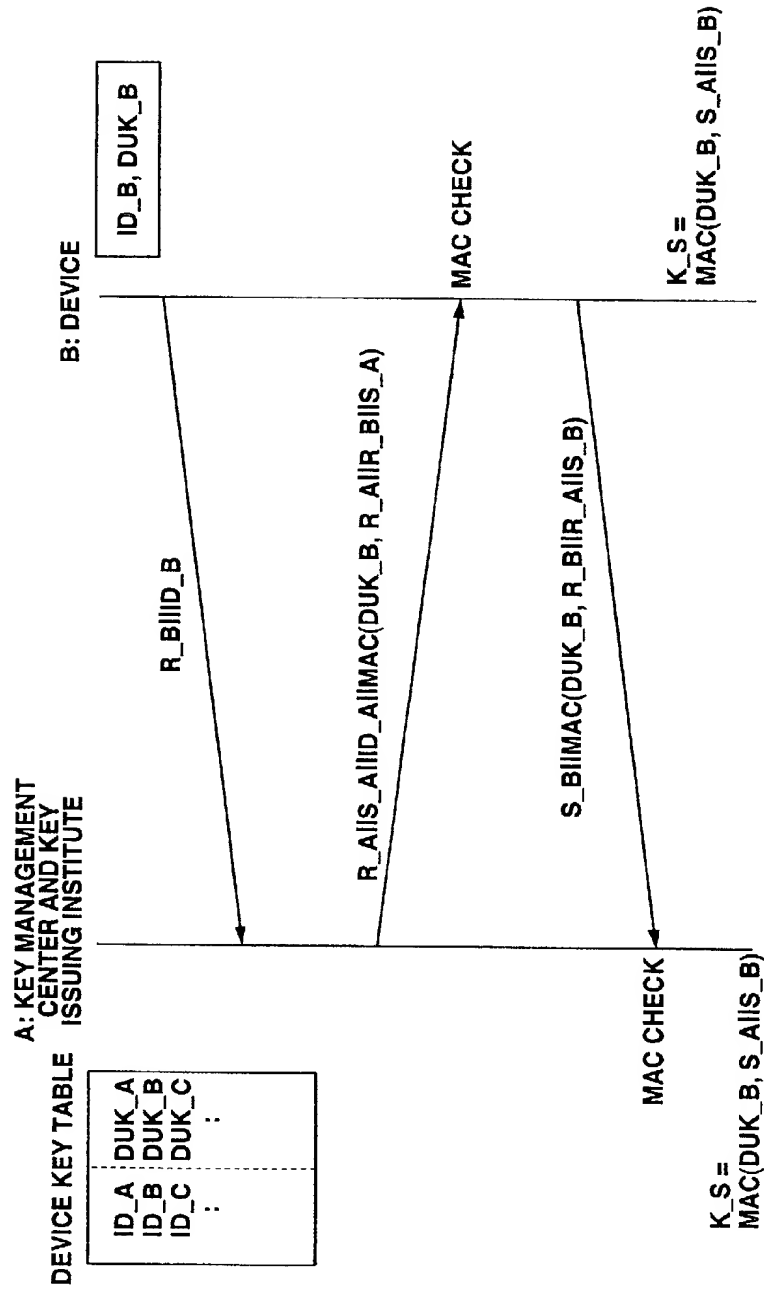


FIG.26



GENERATION #n	
DEVICE UNIQUE IDENTIFICATION NUMBER (DEVICE ID)	ENCRYPTED MASTER KEY
1	Enc(DUK_1, MK_n)
2	Enc(DUK_2, MK_n)
:	:
L	Enc(DUK_L, MK_n)

FIG.28

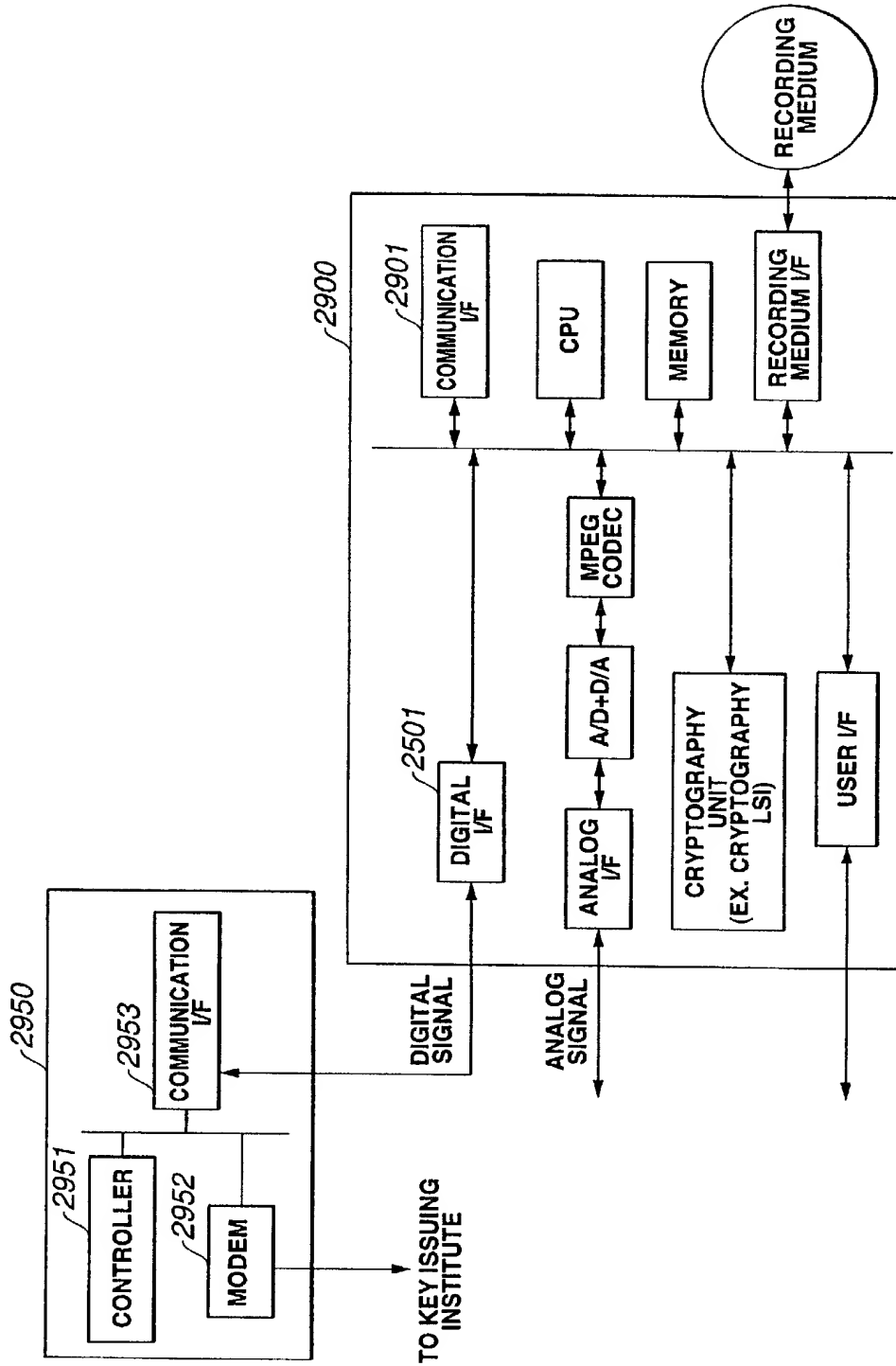


FIG.29

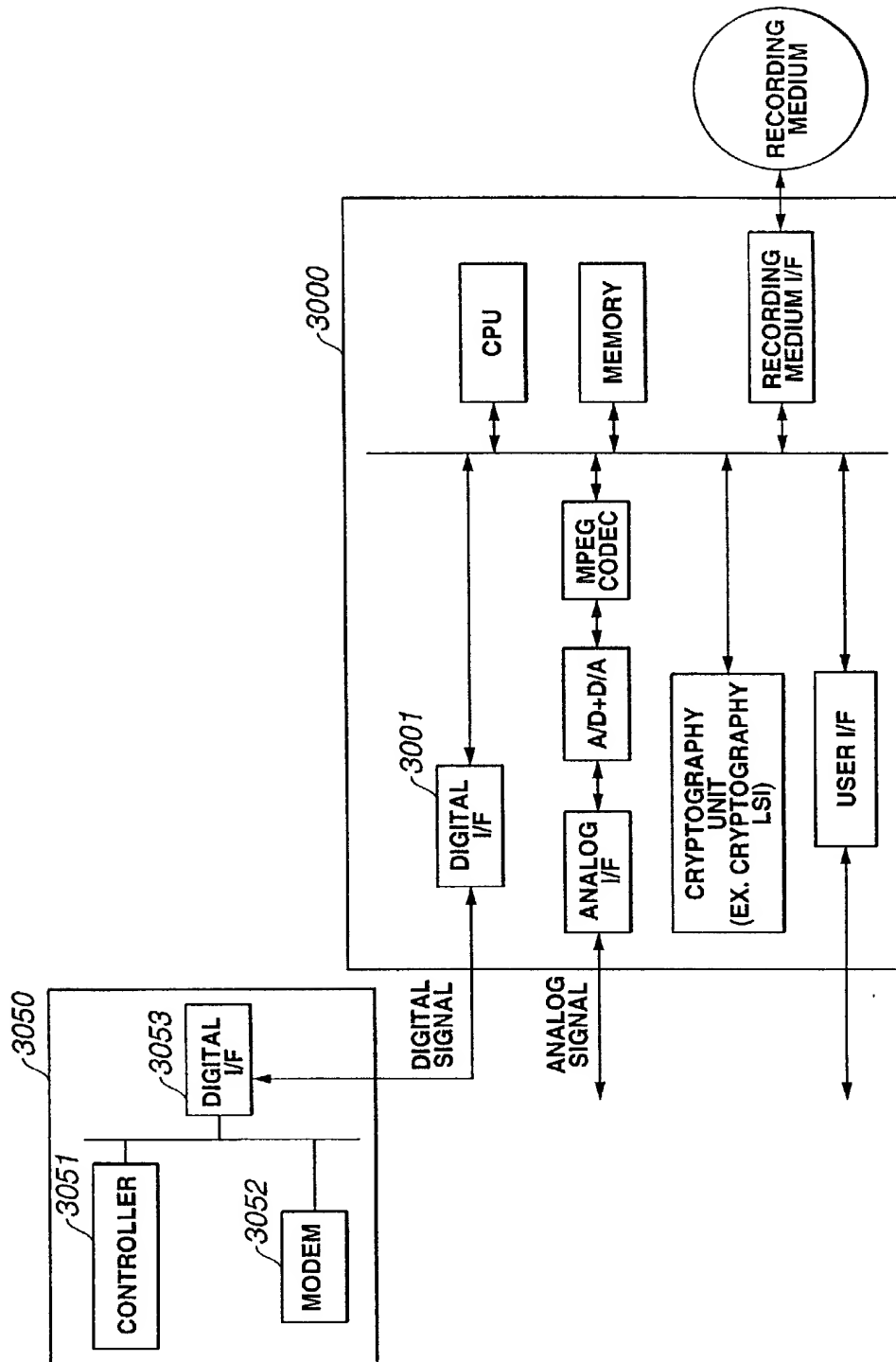


FIG.30

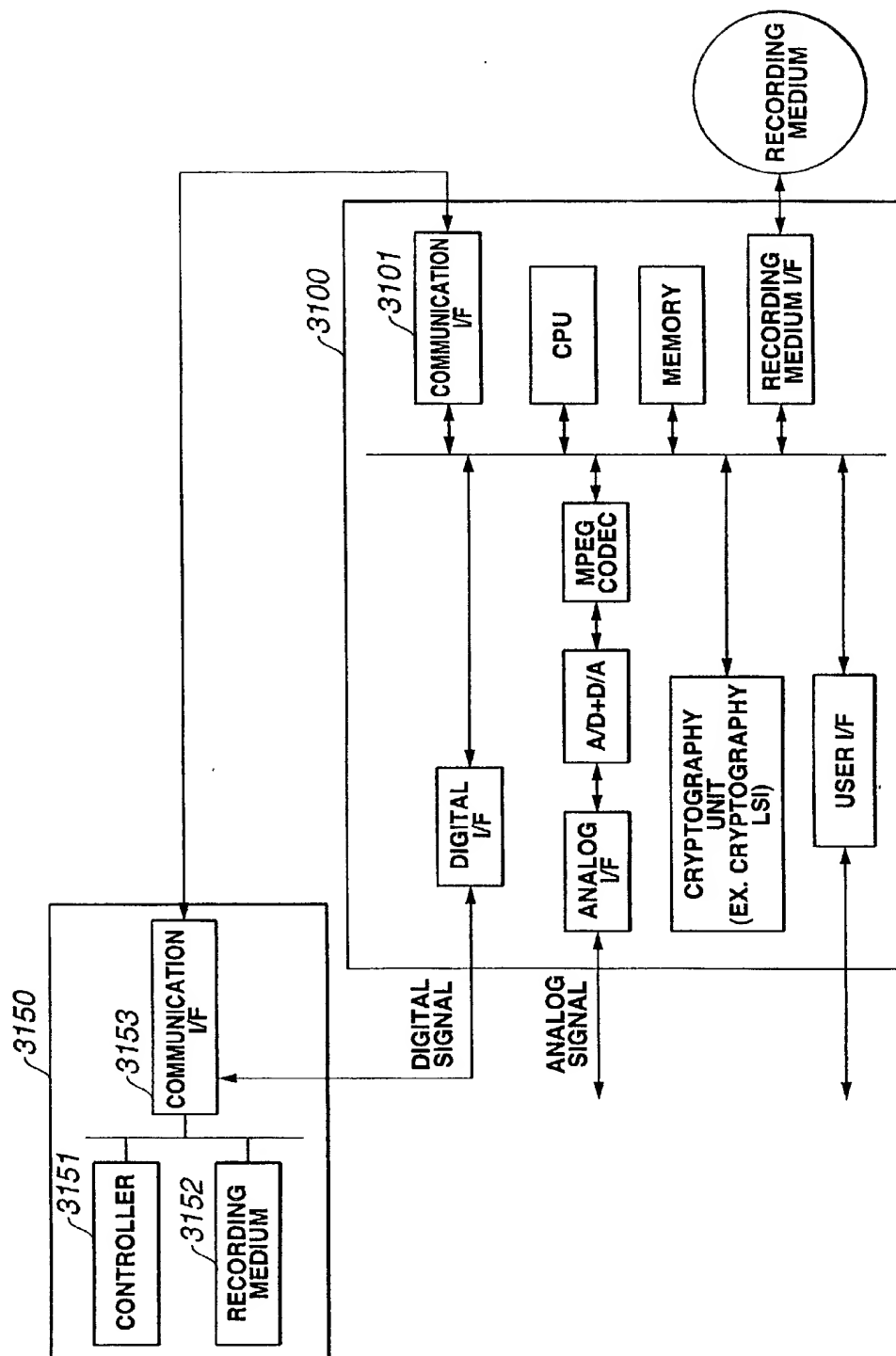


FIG.31

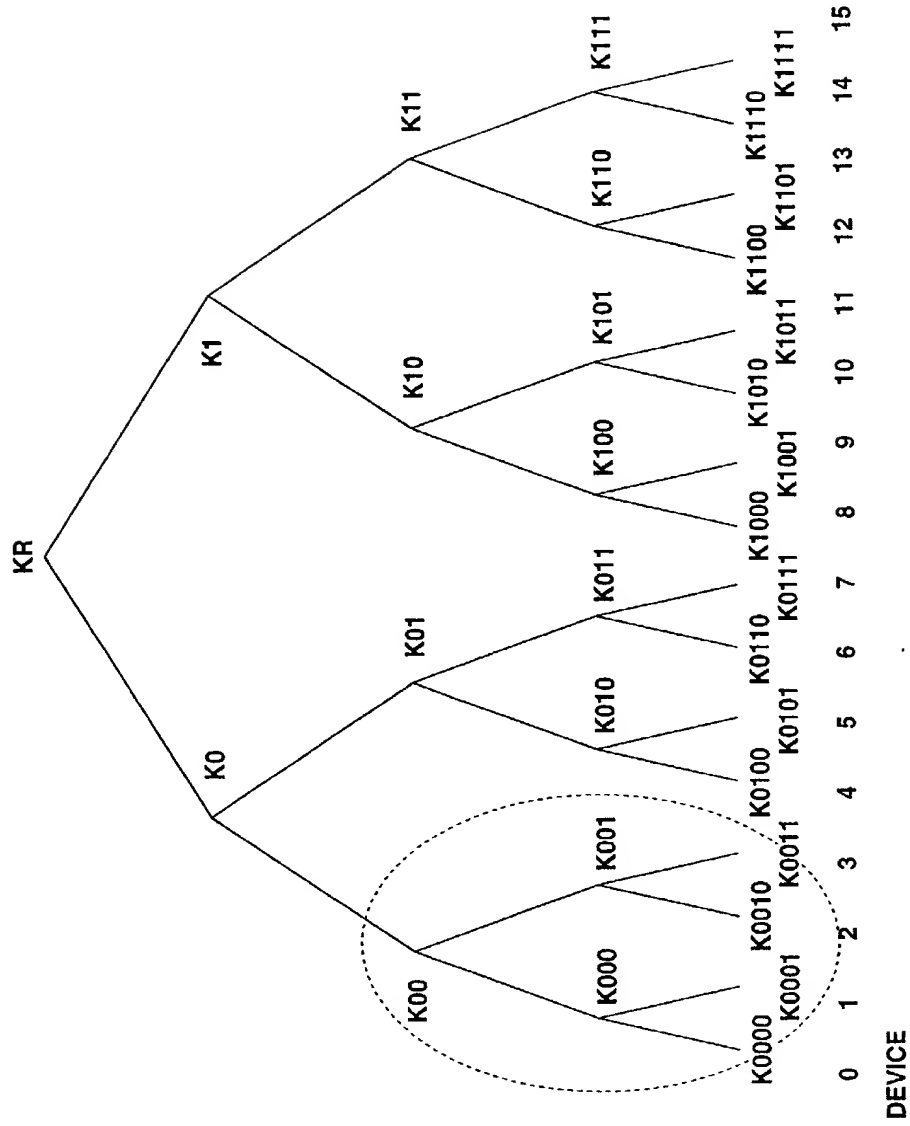


FIG.32

30/37

GENERATION : t	
INDEX	ENCRYPTION KEY
0	$\text{Enc}(K(t)0, K(t)R)$
00	$\text{Enc}(K(t)00, K(t)0)$
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$

**FIG.33A**

GENERATION : t	
INDEX	ENCRYPTION KEY
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$

**FIG.33B**

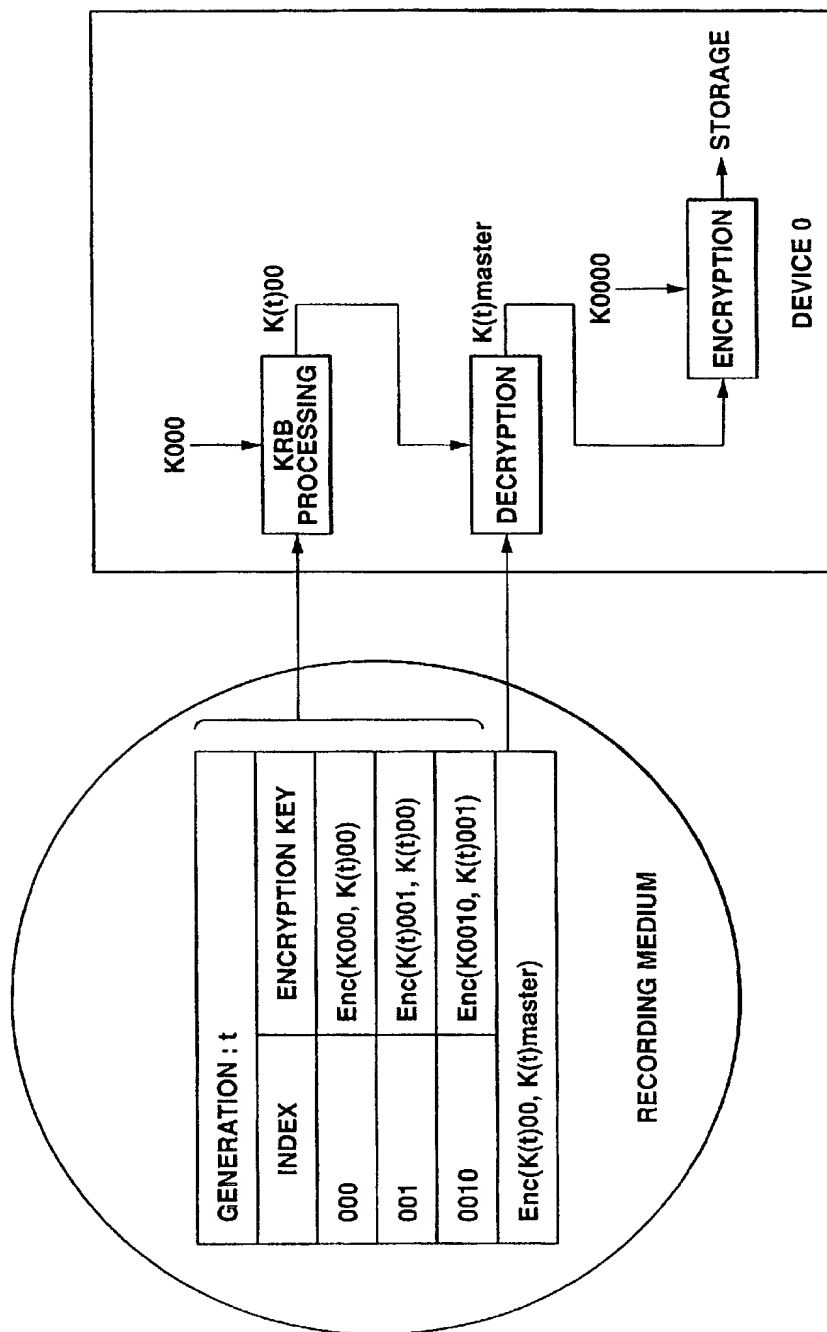


FIG.34

32/37

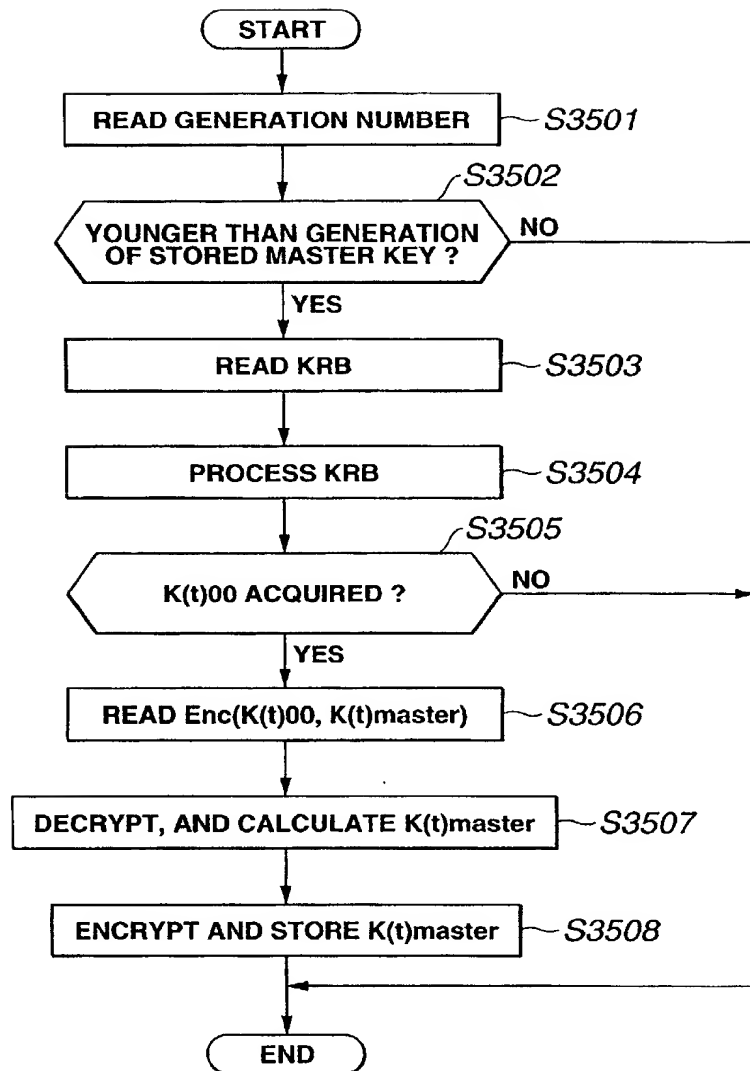


FIG.35



34/37

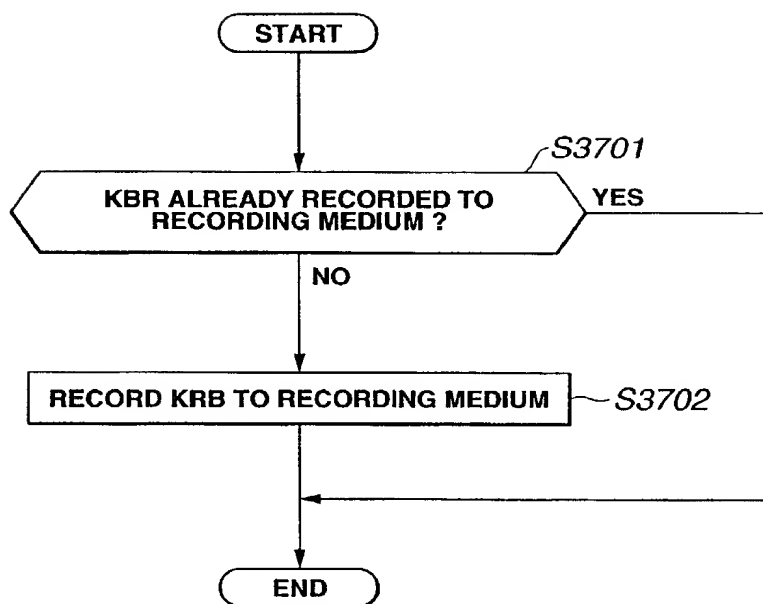
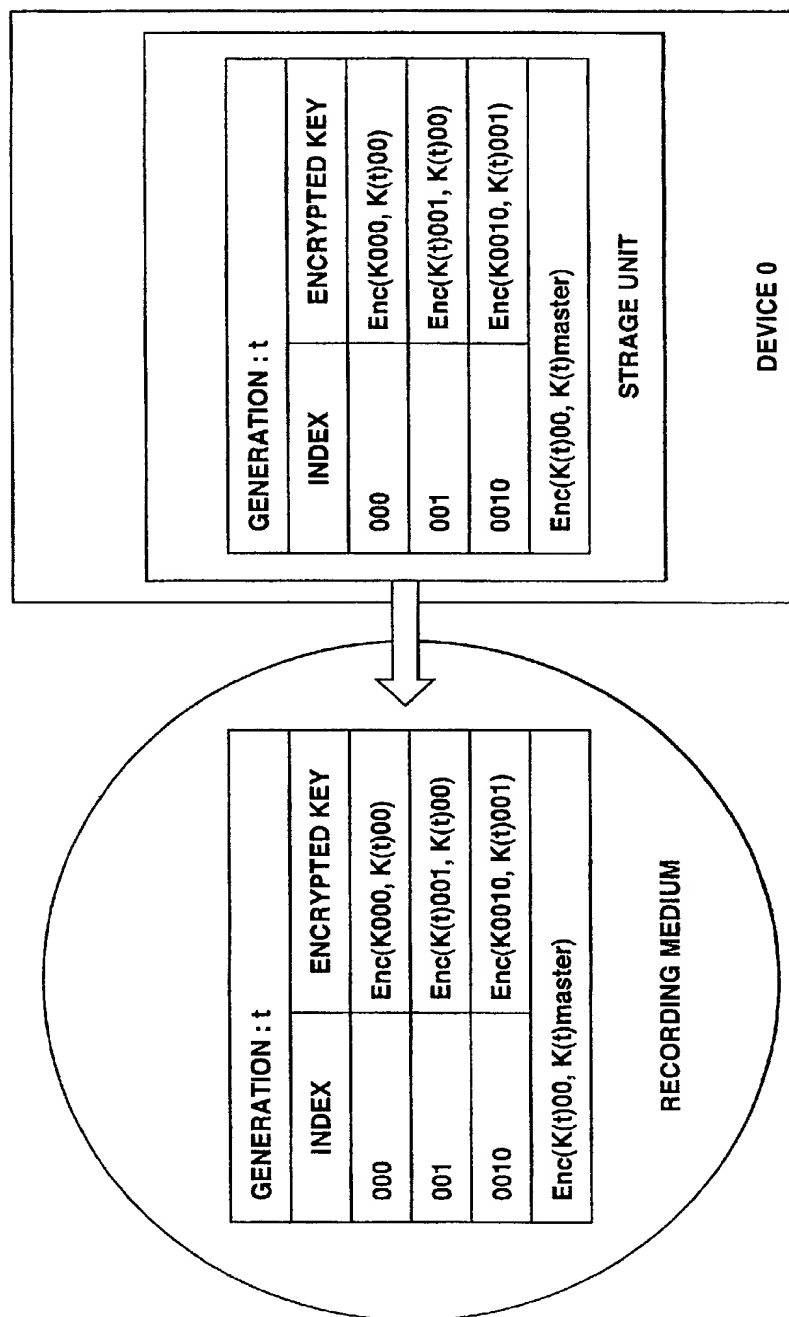
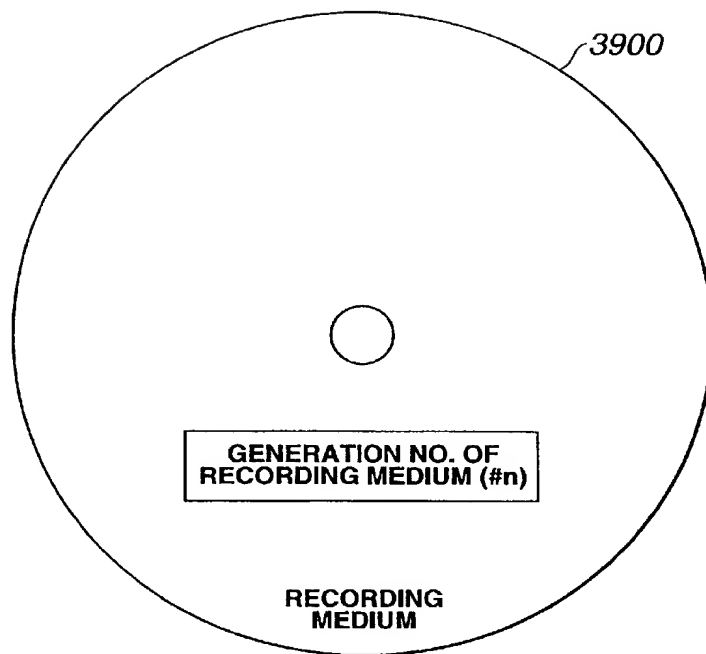


FIG.37

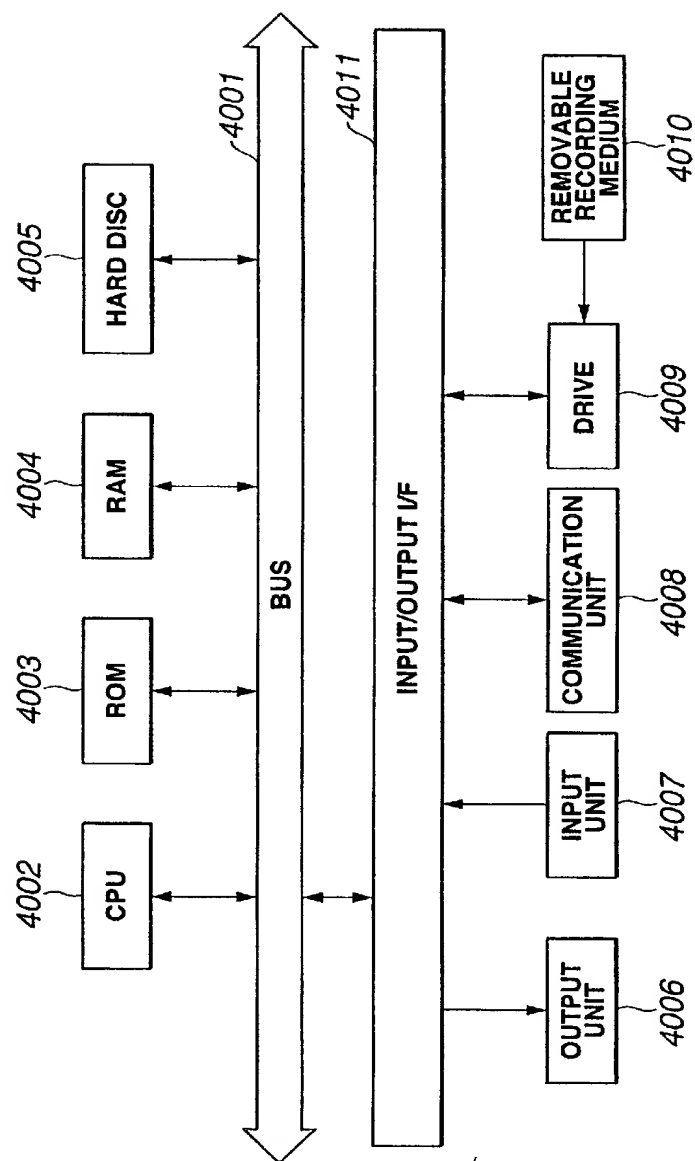


**FIG. 38**

36/37



**FIG.39**

**FIG.40**